EXHIBIT 2

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
WESTERN DIVISION

KAJEET, INC., Plaintiff, vs. QUSTODIO, LLC, Defendant.	CASE NO. 8:18-cv-01519-JAK-PLA **JURY TRIAL DEMANDED**

DECLARATION OF DR. CHARLES D. KNUTSON IN SUPPORT OF PLAINTIFF'S RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS

Dated: December 20, 2018

Charles D. Knutson

I. INTRODUCTION

1. My name is Charles D. Knutson. I am over 18 years of age and competent to testify to the facts stated herein. I have personal knowledge of the facts stated herein. I declare under penalty of perjury under the laws of the United States that they are true and correct.

2. The following statements set forth my opinions in the above-referenced matter relating to the patent eligibility of the claims of the Patents-in-Suit, and the basis for them. The statements expressed herein do not constitute an exhaustive discussion of each and every detail that relates to or supports my opinions. As such, I reserve the right to explain and support my opinions further. I also reserve the right to supplement, alter or modify my opinions if necessary to respond to additional positions taken by Defendant Qustodio, LLC.

A. Scope of Engagement and Compensation

3. I was retained by the law firm of Friedman, Suder & Cooke, P.C. ("FSC") on behalf of their client Kajeet, Inc. ("Kajeet"), to provide expert analysis and to opine on subject matter relating to the patent eligibility of the claims of the Patents-in-Suit.

4. I have been asked to submit my opinions on the disclosure and claimed inventions of the Patents-in-Suit, the problems solved thereby, the

technological advancements giving rise to those problems, and what was routine, conventional, and/or well-known in the art of mobile communication device controls at the time of invention.

5. Under the terms of my agreement, I am being paid an hourly rate for my services, plus necessary and reasonable reimbursements related to the services provided. I will receive no other compensation for my work. I have no financial interest in the outcome of this case, and my compensation is not dependent in any way on the outcome of this case.

B. QUALIFICATIONS

6. I received my Doctor of Philosophy (Ph.D.) degree in Computer Science from Oregon State University in 1998. I received my Master of Science (M.S.) and Bachelor of Science (B.S.) degrees in Computer Science from Brigham Young University (1994, 1988). I have been engaged in the software development industry since 1986 in engineering, management, research, and instructional positions. I was employed at Hewlett-Packard and Novell, Inc. from 1988 to 1994, developing data communications software and systems.

7. I have been a Computer Science faculty member at Oregon State University (1999 to 2000), Brigham Young University (2000 to 2014), and Utah Valley University (2018 to present). I am currently an Emeritus Professor of

Computer Science at Brigham Young University and an Associate Professor of Computer Science at Utah Valley University. I founded the Mobile Computing Lab at Brigham Young University in 2000, conducting research in wireless data communications and mobile computing platforms and systems. I developed and taught courses at BYU in wireless data communications, social network analysis, social media, and ethics and computers in society.

8. Between August 2007 and 2010 I developed and taught parenting classes on online safety at BYU's Campus Education Week. In September 2007 I founded the Internet Safety Podcast, which became the most popular podcast on the subject of Internet Safety on iTunes at the time. In 2012, I founded the Internet Safety Project as a non-profit corporation dedicated to helping parents, leaders, and educators protect children online. Since 2007, I have given more than 50 public presentations, including multiple television and radio appearances, on the subject of online safety, primarily focused on keeping children safe in the emerging landscape of digital connectivity. I wrote a book on Internet safety published in 2014, targeted to parents and leaders of my religious faith, entitled *Digital Mists of Darkness*.

C. DOCUMENTS REVIEWED

9. In preparation for providing the opinions expressed herein, I have reviewed the Patents-in-Suit and their respective file histories, the Complaint in the above-styled action, and Qustodio's Motion to Dismiss (Dkt. No. 37). I have also had discussions with litigation counsel for Kajeet to discuss the law on subject matter eligibility for patenting.

10. Further, I have consulted numerous publications (including a number of books) on data communications, networking, security, and computer science. I have also consulted numerous publications (including a number of books) on online child safety, digital parenting, pornography addiction, gaming addiction, online predators, Internet filtering, parental controls, and other related topics. I have also consulted numerous presentations and talks given around the time frame of the filing of the Patents-in-Suit. Among the books and presentations I consulted were publications that I have authored, public presentations I have given, slides for public presentations I have given, and interviews I have been involved in (both as interviewer and interviewee) concerning the subject matter of the Patents-in-Suit.

II. THE EMERGENCE OF SMART MOBILE DEVICES

11. The IBM Simon is typically credited as the first commercially viable mobile smartphone device, released initially in 1992 as "Angler" and then again in 1994 after further refinements (and a rebranding as "Simon"). The release of the

IBM Simon coincides closely to the time period in which the Worldwide Web began to find popularity with Netscape's release of Navigator in late 1994. Through the late 1990's various "personal digital assistants" ("PDAs") were released, including the Palm Pilot, the Apple Newton, and the Microsoft Pocket PC. These devices, dubbed "smartphones," expanded the set of features one came to expect from a handheld mobile computing device, even while coexisting in the market with what would come to be known as "feature phones." Apple's release of the iPhone in 2007 signaled the dawn of mainstream smartphone usage, accelerated one year later by the release of the App Store, which revolutionized the ability for users to customize the capabilities of the devices they carried with them.

12. Between 1998 and 2005, the number of households with a cell phone grew from 36% to 71%, according to the U.S. Census Bureau. A study by the Pew Internet & American Life Project found that in 2004, 45% of teens had a cell phone. Pew reported that by 2008, 71% of all teens had a cell phone, compared to 88% of parents. In the decade since that Pew report, cell phone usage among both parents and teens has become essentially universal, and smartphone usage has followed a similar upward trend. Fast forward almost a decade, and a recent Pew study (conducted in 2015), now shows that 24% of teens are online "constantly," with 92% of teens reporting going online daily. Nearly 75% of teens either own a

smartphone or have access to one. (Teens, Social Media & Technology Overview 2015) The remaining minority undoubtedly have traditional feature phones, with only a small sliver of the teen population in the U.S. having no access to any cell phone at all.

13. The advent of ubiquitous mobile devices in the hands of children and youth created a significant shift in the social fabric for kids, especially as traditional parenting and teaching strategies intersected with new technical realities, frequently with disastrous consequences. As teens became perpetually connected, a wide range of new problems emerged, many of them unprecedented in the experience of the parents, teachers, and ecclesiastical leaders trying to help teens. Among these new Internet-fueled and technology-enabled struggles were the following: 1) Internet pornography; 2) Online predators; 3) Identity theft; 4) Cyberbullying; 5) Sexting; 6) Online gaming addiction; 7) Email dangers, including phishing attacks, email scams of varying types, and new avenues for predators to access children; 8) Cybercrime of various types, including credit card theft; and, 9) Viruses and malware. This list is just the tip of the iceberg of what was unleashed on society when we shifted to a new reality in which every teen could potentially be digitally connected, not only to all of their friends, but to *literally every person and place on the planet at any time, day or night*.

14. As an example of the reality shift created by the advent of ubiquitous digital connectivity, Mark Kastleman describes what he calls, "The Four A's of the Internet" (Mark B. Kastleman, *The Drug of the New Millennium*, 2007). Kastleman's focus is Internet pornography, so the descriptions below pertain specifically to pornography. The applicability of these principles to other online child safety concerns is obvious.

- Accessible: Online pornography can be accessed 24/7 on a phone that lives in a backpack or a back pocket. No trip to an adult bookstore in the seedy part of town, and no ID required to obtain illicit material.
- Affordable: Significant pornographic content is available online, to anyone, for free. Producers of pornography give significant content away because, as the drug dealer's motto states, "The first one is free."
- Anonymous: Accessing online pornography is, for the most part, socially anonymous. There is no need to risk having one's car spotted in the parking lot of a strip club when you can access the same material whenever you find a moment of privacy.
- Aggressive: Even if you have every intention and motivation to avoid online pornography, you will almost certainly be exposed to it online because producers of illicit content don't simply wait for you to stumble

by – they aggressively go after new users, knowing that once a user, especially an adolescent, is exposed to pornography, their brains will naturally want to see more.

15. The social, emotional, economic, spiritual, and physical dangers placed in the path of our children by the advent of ubiquitous mobile devices is unprecedented in the history of humanity. The best parents in the world could not simply take the conventional wisdom of their childhoods in the 50's, 60's and 70's and thereby be an effective parent facing this modern problem. This is a problem rooted in advances in technology that requires a solution similarly rooted in technology. Old paradigms do not suffice.

III. PRIOR ART MEANS OF COMMUNICATION DEVICE MANAGEMENT

16. The known systems and methods for control prior to the time of invention were largely inadequate and relied upon 1) denying a child all access to a communication device in order to prevent disallowed usage and/or 2) storing control policies locally on the communication device itself within accessible portions of the device's memory. Solutions such as these were entirely inadequate to address the new parenting realities of a digitally connected generation of teens since they were ineffective at preventing unapproved or unsafe use and therefore

were tantamount to taking the phone away altogether, rather than providing an effective (and selective) control mechanism to promote safe use of the device.

17. These first solutions offered no granularity to a parent or employer to control access to specific functions while allowing access to the device. Further, they were ineffective because control mechanisms and policies were locally accessible through the device itself, and hence were vulnerable to manipulation by the user. These solutions additionally suffered from high administrative overhead since each communication device required separate and independent configuration by an authorized administrator.

18. Kajeet addressed these shortcomings through the use of a distributed architecture scheme in which usage policies were stored remotely from the controlled communication device. This approach made it much more difficult, if not impossible, for users to access and manipulate security settings, resulting in a more effective control scheme, while also accommodating real-time control of user groups (consisting of one or more devices for which a common set of security policies could appropriately be applied). These represented technological improvements to the operation of communication device control systems and methods.

IV. THE PATENTS-IN-SUIT

19. The Patents-in-Suit comprise U.S. Patents Nos. 3,712,371, 8,667,559, and 8,360,612. These three patents share a common specification and are part of a larger family of thirty-two issued patents assigned to Kajeet. I understand that the common specification of the Patents-in-Suit discloses how the proliferation of cell phones and other modern communication devices throughout aspects of modern life created the problem of providing adequate control over these devices, encompassing a wide range of functionality accessible at any time from virtually anywhere. *See, e.g.*, '371 Patent at 1:37-56.

20. The specification makes clear that the problem to be solved is how to maintain effective control to prohibit certain uses while still allowing approved uses, all in the context of the user possessing the device at all times, including when physically apart from and/or not in contact with the parent/administrator. *See, e.g.,* '371 Patent at 2:7-21; *See, also,* '371 Patent at 3:24-29; 5:14-19; 12:47-67. Kajeet solved these problems through the remote storage of usage policies which are thereby less vulnerable to manipulation by the device user, at the same time accommodating real-time, continuous control concurrent with device usage, which improved the functionality of computer-based systems through improved security, effectiveness, and robustness of control.

21. The requirement for remote policy storing is implicit in claim 1 of the '371 Patent. Claim 1 requires that "requests" to use certain functionality of a computing device ***be routed via a switch or node to a policy decider module*** and that ***decisions be transmitted back through the switch or node for enforcement*** on the controlled device. These limitations capture the distributed architecture scheme of the Patents-in-Suit. Similar limitations, among others, are present in claims 13, 22, and 27 of '371 Patent. Inclusion of such limitations within the claims captures at least the distributed architecture arrangement and results in the claim being confined to a particular solution within the corresponding technical field rather than being directed merely to the broader abstract concept of applying parental or corporate policies to control access.

22. The requirements for storing policies remotely, as well as real-time application of usage policies are included within the limitations of claim 27 of the '559 Patent. That claim requires that "requests" to communicate with remote computing devices be ***sent to a server*** from which a decision on the request is provided ***in real-time***. Similar limitations, among others, are present in claims 1, 13, and 22 of the '559 Patent. Inclusion of such limitations within the claims captures at least the distributed architecture arrangement and results in the claim being confined to a particular solution within the corresponding technical field

rather than being directed merely to the broader abstract concept of applying policies to control access.

23. The requirements for remote policy storing as well as application of a single set of policies to a group of devices are included within the limitations of claim 1 of the '612 Patent. This claim requires ***grouping of the managed computing devices, associating policies to the devices by group*** and that enforcement of policy decisions include ***sending data corresponding to the decision back to the managed device(s).*** Similar limitations, among others, are present in claims 13, 22, and 27 of the '612 Patent. Inclusion of such limitations within the claims captures at least the distributed architecture arrangement and results in the claim being confined to a particular solution within the corresponding technical field rather than being directed merely to the broader abstract concept of applying policies to control access.

24. The claims of the Patents-in-Suit are rooted in control schemes for managing mobile communication devices and require remote storage of usage policies which are thereby less vulnerable to manipulation by the user of the device(s) being managed while still accommodating real-time control concurrent with device usage. The claimed systems improve the functionality of the computer-based systems through improved security, effectiveness, and robustness

of control accommodated. As such, the claims are directed to patent eligible subject matter at step one.

25. Defendant's parenting analogy purportedly reading on claim 1 of the '371 Patent suffers from a host of deficiencies, including (but not limited to):

- Defendant's analogy is premised on absurd reductions or omissions of claim elements from claim 1 to make the analogy work, such as identifying the parent as being the "switch or node" as well as the "policy decider" *and* "policy enforcer" while ignoring limitations directed to the interactions between those elements that implicate structural limitations on the claimed system's architecture. Other examples include conflating a decision to deny access with the enforcement of that decision.
- Several claim terms are well-known terms of art in data communications and security (such as "receive," "send," "request," "store," "data," and "policy"), and yet Defendant ignores these well-known meanings appropriate to the context of the patent claims, and instead acknowledges only such meaning as might occur in common parlance, effectively stripping away all technical aspects of the claim that clearly places it within a particular technological field; and,

- The patent requires that the request is sent from the device, rather than from the user of the device. As an example, the patent is clear that the "request" sent by the device and received by the server occurs as a transmission of data packets from the client (the user device) to the server across a data communications link (such as the Internet).

26. Defendant's analogy also fails to appreciate the true scope of the problem addressed by the Patents-in-Suit as well as the language of the claim requiring that the policies be operable to control "requests ***to or from*** the computing device." In modern mobile communications devices, use can be proactive or reactive – meaning communications may be initiated by the controlled device or by remote devices reaching out to the controlled device. The parenting example set forth by Defendant does not address this concept and is unworkable to provide control over incoming communications in the manner contemplated by the Patents-in-Suit, namely policy enforcement by a server that constrains the ability of the device to receive data transmissions consistent with the "request" issued by the device. Such a "request" may or may not coincide with a specific action on the part of the user. Imagine, for example, that a child goes to a site on the browser in their phone. That page loads, and while not caught by the web filter, turns out to be malicious. After loading, the webpage immediately redirects the browser to a

pornography website, for which the child performed no action, and did not try (or even want) to see. In this instance, with no involvement on the part of the child, the browser makes a forbidden request at the behest of a remote communication device. Defendant's analogy fails entirely to contemplate this scenario which is all too common in the real world, and clearly anticipated by the Patents-in-Suit.

27. A system practicing the invention of claim 1 of the '371 Patent would also operate to receive the request from the browser ***directed to the child's phone*** and deny it, in order to protect the child from this harmful content that came looking for the child (not the other way around). This notion of inappropriate and harmful content (especially, but not exclusively, pornography) aggressively coming after a child is a significant area where Defendant's parental analogy completely breaks down. This is just one example of many that could be provided illustrating that in the context of modern communications devices, and the network access they accommodate, inappropriate access to content by children is oftentimes unintentional. Defendant's analogy does not account for this because it is premised on a lack of appreciation of the problem addressed by the Patents-in-Suit and partakes of an oversimplification of the corresponding solution claimed.

28. Defendant's analogy relating to claim 27 of the '559 Patent and Claim 1 of the '612 Patent likewise suffers each of the same deficiencies as discussed

above with respect to claim 1 of the '371 Patent and therefore fails to present a real-world analogue to the claimed inventions as Defendant contends.

29. When considered as an ordered combination of elements, the challenged claims comprise an "inventive concept." Each requires storing usage policies remotely from the managed devices, an unconventional arrangement at the time which yielded improvements in the operation of such systems. As noted above, I am aware of few communication device controls that were available at the time of invention of the subject matter claimed in the Patents-in-Suit. Each of these systems relied on storing settings and policies within accessible portions of the device's memory. As such, these policies were accessible to users of those devices for manipulation and/or deactivation or deletion, circumventing the control system entirely and requiring that each communication device be separately configured. The arrangement disclosed and claimed in the Patents-in-Suit runs counter to what was well-known, routine, or conventional at that time by requiring remote storage of such policies while effecting real-time control over communication devices and providing other benefits, as discussed above.

30. As a person of ordinary skill in the art, I recognize this claimed arrangement as placing meaningful limitations on the scope of the claims relating

to how they solve the problem, rather than broadly claiming an abstract concept which may be applied to solve the problem.